EXHIBIT 137

NATIONAL AUTOMOBILE DEALERS ASSOCIATION
8400 Westpark Drive • McLean, Virginia 22102
703/821-7040 • 703/821-7041

Memo

To: NADA Members

From: NADA Legal and Regulatory Affairs

Date: August 28, 2013

Re: Dealer Data Guidance – Sample Service Provider Contract Language

---

Dealers collect a large volume of information from their customers in their day-to-day operations, with much of that information categorized under federal law as highly sensitive "non-public personal information" or "NPPI." What information is NPPI is a complicated topic, but generally speaking, NPPI is any personal information that a dealer collects about an individual in connection with providing a financial product or service, that is not otherwise "publicly available."[1] This could include information such as that contained on an individual's credit application or credit report,[2] but it could also include any information that identifies that individual as having financed or leased a vehicle, such as APR, down payment, or monthly payment.[3]

This is important because the information's status as NPPI means that the dealer is subject to several obligations under federal law to protect and maintain its privacy. Even customer information that does not rise to the level of NPPI can be sensitive to the consumer and the dealer and thus should be protected closely by dealers. In addition, this customer information has tremendous commercial value to the dealer and could be deemed to be a trade secret under state law.[4] Of course, this data has value to others as well and, as a result, there are a number of entities who wish to gain access to the data.

This customer data is generally stored in the dealer DMS and related computer systems, along with a great deal of other sensitive financial data about the dealership and its employees. In today's world of online commerce, dealers, like many other small businesses, rely on a number of third party service providers to store the data or provide technical or other services

---

[1] *See, e.g.*, http://ftc.gov/privacy/glbact/glboutline.htm

[2] This could include information such as name or address if obtained via that application or report. This creates obvious difficulties when seeking to limit "sharing" of NPPI by data field.

[3] For more on finance or lease "identifiers" and why they are NPPI, see "A Dealer Guide to the Privacy Rule and the Model Privacy Notice" at www.nadauniversity.com.

[4] While each state has its own laws relating to trade secrets, a customer list or other data may be deemed a trade secret in certain circumstances although you generally have to show that you have taken steps to keep the information secret. This is yet another important reason why you want strict controls over who has access to your customer data.

that require access to certain data in the dealer DMS. The result is that this customer and other sensitive data (together "Dealer Data") raises difficult and sensitive issues for dealers that they must understand when they enter into contracts that could allow access to Dealer Data.

The basic problem is the inherent conflict between, on the one hand, the need to provide access to manufacturers, vendors, and other third parties who legitimately require access to portions of the Dealer Data so that they can provide a service to the dealer, and, on the other hand, the dealer's regulatory duties regarding the Dealer Data, as well as their legitimate business interests in the Dealer Data.

To properly manage this conflict, dealers must (1) understand the issues at stake; (2) understand who is seeking to access their Dealer Data, and why; (3) control and monitor that access, and (4) ensure that the contracts governing that access address the relevant issues and contain the appropriate language to protect dealers' business interests and regulatory responsibilities.

This memo does not, and is not intended to, provide legal advice, nor advice about the business issues in dealers' vendor or other contracts. Instead, it is intended to highlight several recurring issues in contracts implicating access to Dealer Data, and the federal regulatory issues raised by them. Dealers must consult with their own counsel with respect to all contracts, as well as all federal, state, and local regulatory obligations.

The Regulatory Requirements

Details about the underlying regulatory requirements are complex and largely outside the scope of this memo. Dealers should review the numerous dealer guides available at www.nadauniversity.com covering the relevant federal regulatory issues including the GLB Safeguards Rule, GLB Privacy Rule and Model Privacy Notice, the Affiliate Sharing and Marketing Rules, as well as telemarketing and other guides for more details about the various rules affected by sharing or allowing access to Dealer Data, and associated issues potentially implicated by certain types of service provider contracts.

However, given the need to understand at least the basic issues at stake in order to grasp the implications of certain contractual provisions, keep in mind that dealers' duties with respect to Dealer Data are governed by two primary federal regulations – the Safeguards Rule and the Privacy Rule.[5] Broadly speaking, the Safeguards Rule requires dealers to take certain procedural and technical steps to ensure that certain customer data is protected from inadvertent disclosure or other access by third parties (such as theft, hacking, etc.) who could then use the information to steal an individual's identity or otherwise harm the consumer. Similarly, the Privacy Rule is intended to protect consumers' financial privacy and prohibits dealers from sharing NPPI with any third party unless (1) an exception applies, or (2) they first provide the customer with a privacy notice and allow the customer the chance to opt out. Dealers must also provide their customers with a notice informing the customer of their information sharing practices.[6] As a practical matter the overwhelming majority of dealers provide a notice that

[5] These are the shorthand names for two regulatory provisions under the Gramm-Leach-Bliley Act ("GLB").

[6] The FTC's Model Privacy Notice includes all the required notices in one form.

states that they do NOT share NPPI with any third parties.[7] Of course, this means that dealers must honor the promise not to share the customers' data.

An important issue to understand is that the FTC may consider any third party "access" to NPPI to be the equivalent of "sharing."[8] In other words, if a third party has access (via your computer network or otherwise) to NPPI or *could* access it, you may be deemed (or at least alleged) to have "shared" that data, even if the third party never actually accesses, obtains, processes, or relies upon the data.[9]

"Service Providers"

Another important issue you must understand under both the Safeguards and Privacy Rule for the purposes of this memo is that of the "service provider." The federal regulations contemplate that entities will use the services of third parties, and may need to share or otherwise expose NPPI to those third party service providers. Section 313.13 of the Privacy Rule contains one of the "exceptions" mentioned above, and allows a dealer to share NPPI with a service provider without providing the required opt-out opportunity described above,[10] but *only if you do so pursuant to a contract* that puts specific restrictions on the service provider. The idea is that you can provide access to the sensitive information, but *only* to the extent needed to provide the service and that service provider cannot then use or share the information with anyone else.

The Safeguards Rule also contemplates the use of service providers, but again, only subject to restrictions. Under the Safeguards Rule, the dealer must (1) "[t]ak[e] reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue"; and (2) "[r]equir[e their] service providers by contract to implement and maintain such safeguards." In addition, the FTC states that you must also "oversee their handling of customer information."[11]

The Safeguards Rule defines "service provider" as "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a [dealer subject to the Rule.]." This definition would include third party vendors including DMS providers, and in some circumstances could also include your manufacturer.

---

[7] The reasons for this are generally outside the scope of this memo. However, it is important to note that even if a dealer were to provide notice that it will share NPPI, it must also provide a reasonable opportunity for the individual to opt-out of that sharing. The FTC considers 30 days to be a minimum reasonable period. As a result, even if dealers were to share, they would have to ensure that they would not do so for 30 days after gathering the NPPI. As a practical matter, this would be difficult to implement, and would in many cases make the sharing of the NPPI commercially and practically unfeasible in the service provider context.

[8] NADA does not necessarily share or endorse this position, but it is important to understand what the agency's position is likely to be, and in terms of protecting yourself in your contracts you should understand this reality. Whether it is technically "sharing" under the federal regulatory requirements or not, there are good business and practical reasons to understand (and limit) third party access to your data.

[9] As noted below, the definition of "Service Provider" under the Safeguards Rule includes any entity "that receives, maintains, processes, or otherwise is permitted access to customer information."

[10] You must still provide the privacy notice, and if appropriate, that notice must disclose that you share with service providers.

[11] See http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule

The Problem

The primary issue under these federal regulations generally arises because of a disconnect between the duties dealers have and the promises they may have made to their customers, and the demands for access to Dealer Data sought by third parties. While every situation is different, the basic issue can arise in one of several ways. For example:

(1) The dealer wishes to engage the services of a third party service provider that requires access to Dealer Data to perform the service, but fails to ensure that the appropriate contractual provisions and other restrictions are placed on the service provider with respect to Dealer Data.

(2) A manufacturer establishes a marketing or other "program" that either directly or utilizing the services of a third party service provider requires dealers to allow access to Dealer Data, and the dealer either fails to ensure, or is prevented by the manufacturer (or its service provider) from ensuring that the appropriate contractual provisions and other restrictions are placed on the service provider.

In either event, the result is often that Dealer Data, potentially including NPPI, could be "accessed" or "accessible" to the third party vendor, and the dealer runs the risk of violating its Privacy Notice promise to its customers, its Safeguards Rule duties,[12] as well as potential violations under other federal law.[13]

Unfortunately, these scenarios do occur. While the duties and responsibilities are the same, a dealer's response to each scenario is likely to be somewhat different. In the first scenario, a dealer must be vigilant in policing and negotiating their contracts to ensure that the required contractual provisions are included in all service provider vendor contracts. There are a number of other contractual provisions that, while perhaps not required, may be worthy of consideration by the dealer and its attorney in the vendor agreement. We discuss some of those provisions below.

The second scenario often presents more difficult issues for dealers because these manufacturer "programs" are generally presented by the manufacturer to the dealer as, for all intents and purposes, requirements.[14] This means that dealers may in many cases have more limited ability to police and amend these contracts to ensure they are protected adequately against regulatory and other risks. While some contractual protections may be optional, it is

---

[12] In addition, in scenarios involving violations of the Privacy and Safeguards Rules, the FTC will also generally allege a violation of Section 5 of the FTC Act on the basis that a failure to abide by the Privacy Notice promises and the failure to maintain adequate safeguards is "unfair" and/or "deceptive." *See, e.g.* a recent FTC action brought against a dealer, alleging such violations: http://www.ftc.gov/os/caselist/1023094/index.shtm

[13] For example, under the CAN SPAM Act, if a customer opts-out of receiving email from you, you thereafter cannot "sell, lease, exchange, or otherwise transfer or release" that email address to any third party, "including through any transaction or other transfer involving" a list that contains that email address. *See* 15 U.S.C. 7704 (a)(4)(iv). Similar issues arise with phone numbers on your company-specific "Do-Not-Call" list under federal telemarketing regulations. As a result, access to phone numbers or email addresses, even if not NPPI, raise unique and potentially difficult concerns.

[14] For example, dealers may be told that their "participation" in a particular program is required to qualify for certain incentive or other program payments, or that participation is required under the dealer franchise agreement.

important to remember that dealers should not agree to provide access to NPPI, even in these manufacturer programs, in violation of their Safeguards and Privacy Rule responsibilities.

This means that unless their Privacy Notices state otherwise,[15] dealers may not provide access to NPPI to anyone, *including their manufacturer*, unless they do so in connection with a contract (a) pursuant to which the manufacturer is providing a service to the dealer that requires access to the NPPI, and (b) that contains the required contractual provisions (or unless one of the other exceptions to the Privacy Rule applies).[16] NADA understands that this can put dealers in a difficult, if not untenable position. However, it is vitally important, for dealers and manufacturers alike (and ultimately for your customers) that these contractual protections be included. While the dealer is ultimately responsible for protecting and not sharing protected data, regulators and plaintiff lawyers are not likely to hesitate in looking to the manufacturer should a problem arise.

Under both scenarios it is often common for the contracting party to subcontract some of the work; that is, to use another third party to either aid in providing, or to actually provide the service itself. For example, if a third party requires access to the dealer DMS to provide services to a dealer related to their vehicle inventory, they may use another entity to actually interface with the dealer's DMS and "extract" the inventory data that they need. This is important to understand because if you do not ask you may not even be aware that this third party is in your DMS system.[17] And of course, if they have accessed your data, and are not bound by the required contractual restrictions to only take what they require, and not to store, use or share the data, then this can create regulatory compliance and other problems for the dealer (and the service provider and/or manufacturer).

Remember as well that under both scenarios, the third party (and all subcontractors) must also actually be providing the dealer a service and the data that they access must be required to provide that service. That means that you cannot allow access to NPPI just because a manufacturer requests it. For example, you cannot share any information that would identify a customer as a lease or finance customer in a retail delivery report to your manufacturer, unless the manufacturer has a legitimate business need for that information to process the transaction on behalf of the customer (a lease incentive for example.)[18]

It also means that you cannot grant access to NPPI or other sensitive data if it is not required to provide service you have contracted for. For example, if the service provider is providing a service to your parts department that requires access to parts data in your DMS, you generally cannot allow them to have access to your sales records (unless for some reason this information is required to provide the service). This means that you need to (1) understand

---

[15] If the dealer is granting access to NPPI, the required Safeguards and Privacy Rule contractual provisions must be in the contract regardless of the content of their Privacy Notice.

[16] See the NADA Dealer Guide to the Privacy Rule and the Model Privacy Notice for more.

[17] It is also important to understand as part of you obligation to conduct due diligence in selecting a service provider.

[18] It is not enough that the manufacturer itself has a business "need" for the data. This exception only applies if they need the information in order to process the transaction on behalf of *the customer*. If a manufacturer seeks this information, you should try to explain why you cannot share the information. You should also consider asking the manufacturer to explain to you in writing which exception to the Privacy Rule applies to the information they are seeking to obtain and why.

exactly what data a service provider needs to provide the service, and (2) take the appropriate technical steps to ensure that their access is limited to that data and that data only. Remember, it is not only the data they actually take, but the data they *could take* (have access to), that you must control. You should also audit and monitor their access to ensure they are not in breach of the contractual restrictions.[19]

Contract Provisions

As discussed above, dealers must include the required Safeguards and Privacy Rule provisions in all vendor contracts.[20] Attached at Exhibit A are several possible sample contract provisions you may want to include in your service provider contracts to meet the requirements under the Safeguards and Privacy Rules.[21] While every service provider vendor contract is different, several other issues tend to arise in many of these contracts, and dealers should consider addressing them in their third-party service provider contracts. For example:

(1) Restrictions on non-contracting third parties. As discussed above, if the contracting service provider uses the services of another third party and that third party has access of any kind to any of to your Dealer Data, you should ensure via contract that the subcontracting third party also meets the same Safeguards and Privacy Rules restrictions you placed on the contracting party. Without a direct contractual relationship with these third parties, their access could nullify the careful steps you have taken to protect yourself with respect to access by the service provider. There are several ways to accomplish this. One potential approach would be to expressly list the subcontracting third parties in the Safeguards and Privacy Rule provisions and requiring the contracting party to warrant that any third parties with access will meet those contractual requirements.

(2) Requirement to provide reports of data accessed. Given the technical complexity of some of these issues, and the lack of visibility dealers may have in these processes, you may also want to consider asking the service provider via contract to provide you with a list of (1) all data fields that they actually extracted from the DMS or other system, and (2) all data fields they had access to, based on their password. This second issue is potentially more difficult, but remember that if they have access to the data, there is potential regulatory risk for the dealer, even if the vendor never actually obtained or accessed that data. You may want to consider including audit rights that would allow you to confirm the reports from the vendor. The feasibility and utility of this type of provision may be determined in large part by the capabilities of your DMS or other systems. You should work with your vendors to determine the best way to gather this data.

---

[19] Some of these steps are addressed below, but specifically, you could consider steps such as: (a) requiring the vendor to send you a written report detailing the data fields they have access to; (b) seeking annual certifications from your vendors stating that they have only accessed the fields outlined in the report; (c) routinely audit vendor password access, and; (d) work with your DMS and other vendors to audit what third parties have access to your system(s), and what data they are accessing.

[20] From the Privacy Rule perspective, the provision must be included if the dealer wishes to rely on the service provider exception to share the information with (or allow access to) the vendor.

[21] Again, these are examples only. This is not intended as legal advice; you should consult your attorney to finalize the language in your contracts, and to ensure that you have considered all state and local issues.

(3) Data breach provisions. Another issue that dealers may want to consider in any agreement with a service provider that implicates access to Dealer Data is the issue of a state law "data breach." Almost all states have a data breach statute that, broadly speaking requires a dealer to notify their customers if there is a "data breach" involving that customer's personal information. The state law definitions vary, but basically a "breach" is deemed to have occurred anytime there is unauthorized access to the data (*e.g.* a hacking incident) or if the dealer *loses control* of the data (*e.g.* a lost laptop or phone containing personal information.) It is important to note a few things about these statutes, (again broadly speaking because they all vary): (a) that the data does not actually have to be accessed or used improperly, a "loss of control" is all that is needed (that is why lost laptops are the most common types of data breaches); (b) that "personal information" can be much more broadly defined than NPPI under federal law (*e.g.* CA where a name and a zip code may be enough), and; (c) that in most cases a dealer can avoid the duty to notify if the data is "encrypted." It is not always clearly defined in the state statutes what "encrypted" means, however you should nevertheless consider requiring that the service provider "encrypt" any data that is accessed, transmitted, or in any other format where you or they could "lose control" of that data. It is crucial that you work with your counsel to determine your state and local law in this area (and all others addressed in this memo). You may want to consider a provision that addresses who is responsible for customer notification and related duties (and costs) in the event of a breach and you may also want to consider requiring the data to be encrypted.[22]

(4) Regulatory issues where service provided is marketing-related. If the service provider requires access to your Dealer Data in order to provide marketing services to you, a number of other regulatory requirements could arise, and you should consider whether to address them in the contract. For example:

a. if the services include e-mail marketing services, issues could arise under CAN SPAM (governing email marketing);
b. if the services involve phone calls or text messages, the federal telemarketing rules (the TCPA and the Telemarketing Sales Rule) could be implicated, and;
c. if the services include "reputation management" or other services related to social media or customer comments or review, the FTC Guide to Endorsements or Testimonials and related disclosure duties could also be implicated.

Again, these issues are outside the scope of this memo, but it is obviously important in a contract implicating any of these federal duties to work with your attorney to ensure that you are protected in the event of a violation of these or other related duties. For example, if the vendor is making telemarketing calls on your behalf, who is responsible for ensuring "Do-Not-Call" compliance? How will you ensure that the vendor honors your company-specific "Do-Not-Call" list or your CAN SPAM "opt-out" list? At the end of the day, it is the dealer who faces the regulatory risk from non-compliance by the service provider. As a result, it is important again that you work with your counsel to make sure you understand the scope of the services to be performed, and that you work with the service provider to ensure compliance.

[22] You may also want to consider whether your vendor is required to maintain "Cyber Liability" insurance coverage. Broadly speaking, this type of insurance covers the costs associated with a data breach.

(5) License Grant. Generally these vendor and manufacturer service provider agreements will also contain a requirement that the dealer grant the vendor or manufacturer a license to the Dealer Data.[23] Dealers and their counsel should carefully consider the implications of any such grant, and in particular, if the scope of the license grant exceeds the Safeguards or Privacy Rule restrictions, it could create regulatory risk for the dealer. In other words, if you have the appropriate Safeguards and Privacy Rule provisions that limit access only to what is needed to provide the service, but the agreement also contains a broad license grant that allows access to non-necessary NPPI, it could be problematic.[24] In some cases, a license may be justifiable, but dealers should be careful to ensure that it is needed, and if so, whether the scope of any such license is appropriate.

(6) Description of the Services/GLB Service Provider Agreement. You may want to consider explicitly stating in the contract (a) the services that are to be provided pursuant to the agreement; (b) that the vendor is a "service provider" pursuant to GLB, and (c) the data fields the vendor needs to take (and have access to) to provide the services.

Dealer Data "Checklist"

These are just some of the issues that routinely appear in service provider contracts. Of course there may be others, and dealers must work with their counsel and internal compliance staff to ensure not only that their contracts contain the required protections, but that the dealership's practices and procedures also adequately protect dealer data. In addition to the regulatory duties imposed under the Safeguards Rule, Exhibit B contains a non-exhaustive list of practical and other steps that dealers should consider taking with respect vendor contracts and to Dealer Data more generally. Many of these points raise a number of complicated issues, and as always dealers should work with their attorneys, consultants, IT staff, and vendors to work through and understand the issues presented.

The bottom line is that Dealer Data is sensitive, important, and valuable. You must have a good understanding of what you have, what the rules are, who has access (including any intermediaries who are not parties to the contract), and who is in control of these issues at your store.

[23] In some cases, we have seen vendor agreements include not only exceedingly broad license grants, but also provisions purporting to grant outright ownership of Dealer Data to the vendor. Of course any such provision would be problematic for all the reasons outlined above.

[24] Many of these agreements will also seek to grant a license to Dealer Data that has been "de-identified" and/or "de-personalized." This generally means that the data (which may or may not have been NPPI) has been stripped of any feature that could identify the customer. This raises complicated and important legal, regulatory, and business issues, and you should carefully review any such license grant with your legal counsel.

Exhibit A - Sample Service Provider Contract Provisions:[25]

Here are several possible examples you could use to ensure that you have the contractual language required under the Safeguards and Privacy Rules in your contracts with your service providers. Some provisions in these examples may not be appropriate in every circumstance. These can and should be combined or otherwise modified as appropriate - ***consult with legal counsel about appropriate language to use for your dealership:***

GLB Service Provider Provision: (Example)

Dealer[26] and Service Provider acknowledges that this contract constitutes a service provider agreement between Service Provider and Dealer subject to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq.* ("GLB Act") and its implementing regulations. Service Provider warrants and represents that access to certain customer information is required to provide the services pursuant to this Agreement ("Services"), and agrees that it will only access that customer or other data from Dealer's computer system(s) that it is authorized to access and that is required to provide those Services.

Safeguards – *Required as described above*: (Examples)

1. Service Provider agrees to protect and secure any and all customer and other data it receives or obtains in any way from Dealer pursuant to this Agreement as required under all applicable privacy and data security laws, and to implement and maintain physical, electronic, and procedural safeguards as provided by Dealer from time to time in Dealer's sole discretion,[27] or of which Service Provider is aware or should reasonably be aware of. Such safeguards shall, at a minimum, comply with applicable federal, state and local laws and regulations. The foregoing shall apply to all of Service Contractor's employees, as well as any subcontractors, affiliates, or other third parties with legitimate access to information and data relating to Dealer or Dealer's customers pursuant to this Agreement ("Authorized Third Parties").

---

[25] These are examples only, and you may wish to incorporate some, all, or portions of one or more of these provisions in your service provider agreements. YOU SHOULD CONSULT YOUR ATTORNEY to ensure that all federal, state and local requirements are met.

[26] All examples assume that capitalized terms are defined elsewhere in the Agreement.

[27] With language such as this, it would likely be appropriate for the dealer to have written guidelines establishing certain minimum standards for such a program, and share those standards with the vendor. For example, in a recent action against a dealer, the FTC cited the dealer for failure to institute certain specific practices including a failure to: "(1) assess the risks to the consumer personal information it collected and stored online; (2) adopt policies, such as an incident response plan, to prevent, or limit the extent of, unauthorized disclosure of personal information; (3)use reasonable methods to prevent, detect, and investigate unauthorized access to personal information on its networks, such as inspecting outgoing transmissions to the internet to identify unauthorized disclosures of personal information; (4) adequately train employees about information security to prevent unauthorized disclosures of personal information; and (5) employ reasonable measures to respond to unauthorized access to personal information on its networks or to conduct security investigations where unauthorized access to information occurred." (See here http://www.ftc.gov/os/caselist/1023094/120607franklinautomallanal.pdf.) Dealer vendors should be held to at least the same security standards as the dealer themselves. Consult your attorney, review the NADA Dealer Guide and/or go to http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule for more details.

2. Service Provider represents and warrants to Dealer that Service Provider (and any subcontractors, affiliates, or other third parties with legitimate access to information and data relating to Dealer's customers pursuant to this Agreement ("Authorized Third Parties")) presently maintains, and will continue to maintain and periodically test the efficacy of, appropriate information security programs and measures designed to ensure the security and confidentiality of "Customer Information" (as defined in 16 CFR § 314.2(b)). Such information security programs and measures shall include, at a minimum, appropriate procedures designed to (1) protect the security and confidentiality of such information, (2) protect against anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer of Dealer. Dealer, its representatives and applicable governmental regulators may, from time to time, also audit the security programs and measures implemented by Service Provider pursuant to this Section, and Service Provider shall not impose any fees or charges on Dealer or its representatives in connection with any such audit.

Privacy Rule – *Required as described above*: (Examples)

1. Access to NPPI not required to provide the Service:

Service Provider understands and agrees that it only has permission under this Agreement to access and use that data that is required to provide the Services; those data fields are listed at Exhibit __. In no event will Service Provider access, store, share, disclose, or use any nonpublic personal information (as that term is defined under the Gramm-Leach-Bliley Act) from Dealer. Service Provider also agrees not to access, enhance, sell, store, share, disclose, distribute, create derivate works from, or use any data accessed from Dealer's DMS or other computer system or otherwise received from Dealer ("Dealer Data") for any reason, except as necessary to provide the Services, and only as long as required to provide the Services to Dealer. Service Provider has no ownership or other rights in the Dealer Data, and may not use Dealer Data in any form to append, trigger, update, enhance, or enrich its own data or data service or any third party data service. Dealer, its representatives and applicable governmental regulators may, from time to time, also audit the data accessed by Service Provider pursuant to this Agreement and the use of that data, and Service Provider shall not impose any fees or charges on Dealer or its representatives in connection with any such audit. The foregoing shall apply to all of Service Contractor's employees, as well as any subcontractors, affiliates, or other third parties with legitimate access to information and data relating to Dealer's customers pursuant to this Agreement ("Authorized Third Parties").

2. Certain access to NPPI required to provide the Service:

Service Provider agrees to only access and use that data that is required to provide the Services, and agrees not to access, store, share, disclose, or use nonpublic personal information (as that term is defined under the Gramm-Leach-Bliley Act) received from Dealer except as necessary to provide the Services. Service Provider also agrees not to access, enhance, sell, store, share,

disclose, distribute, create derivate works from, or use any data accessed from Dealer's DMS or other computer system or otherwise received from Dealer ("Dealer Data") for any reason, except as necessary and for the time necessary to provide the Services. Service Provider has no ownership or other rights in the Dealer Data and shall not use Dealer Data in any form to append, trigger, update, enhance, or enrich its own data or data service or any third party data service. Service Provider agrees not to share the password or other access to Dealer Systems with any other party not specifically outlined in this Agreement, and upon termination of this Agreement agrees that it will no longer access any Dealer Systems or Dealer Data, and to return and/or destroy the password. Dealer, its representatives and applicable governmental regulators may, from time to time, also audit the data accessed by Service Provider pursuant to this Agreement and the use of that data, and Service Provider shall not impose any fees or charges on Dealer or its representatives in connection with any such audit. The foregoing shall apply to all of Service Contractor's employees, as well as any subcontractors, affiliates, or other third parties with legitimate access to information and data relating to Dealer's customers pursuant to this Agreement ("Authorized Third Parties").

Third Party Subcontractors: (Example)

Service Provider warrants and represents that it will: (a) only engage the services of a subcontractor, affiliate, or other third party in connection with its provision of services pursuant to this Agreement ("Authorized Third Party") if required to provide the Services; (b) exercise the requisite due diligence in selecting any Authorized Third Parties to ensure that the Authorized Third Parties can and will safeguard any customer or other information in their care; (c) require any Authorized Third Parties by contract, to abide by Subsections ___[*insert Safeguards Rule subsection*], ___[*insert Privacy Rule subsection*],[28] ___[*insert Confidentiality subsection*][29], and any other relevant provisions of this Agreement; (d) specify by contract that all Authorized Third Parties shall have no license or any other proprietary or intellectual property rights in the Dealer Data pursuant to their agreements with Service Provider; (e) ensure that the Authorized Third Party does not access, enhance, sell, store, share, disclose, distribute, create derivate works from, or use any Dealer Data in any way except as required under this Agreement; (e) provide a list of all Authorized Third Parties (explaining data accessed by each and explanation of role) to Dealer for approval, and seek prior written approval from Dealer before altering or adding to that list, and; (e) require Authorized Third Parties to ensure that any Dealer Data that must be transmitted or stored as part of the Service is transmitted in an encrypted fashion, and in accordance with applicable industry security standards.

[28] Insert the Safeguards and Privacy Rule restriction Subsections (such as those in the above examples) that apply to the Service Provider here.

[29] Insert the provision in the Agreement (if any) addressing treatment of Confidential Information.

Exhibit B – Dealer Data "Checklist"

CHECK WHEN COMPLETED

- ☐ Know and understand who is in your systems and what they have access to:
  - Both employees and any third parties
  - Review access to your DMS any and all CRM databases, your websites, etc.
    - Work with your vendors to determine
    - Don't forget CRM or other (non-DMS) databases
      - Could contain NPPI – (*e.g.*, online credit applications) or other sensitive information
    - Websites
      - What Dealer Data is being accessed by third parties from your website?[30]
      - Work with your website provider to ensure protections against scraping /other data collection are in place.
  - Require third parties with access to provide written list of data they have access to and what they have "taken."
  - Work with your DMS provider to ensure proper controls and reporting
  - Review all current and future contracts for required language
    - Understand what they need and why
    - As discussed above, you MUST limit this via contract
    - Audit/confirm/run reports/hold them accountable/and document!
  - Remember that even if it is not NPPI
    - You still must maintain security
      - Customer relations issues
      - Employee issues
      - Non GLB regulatory duties
    - It has tremendous value
    - Trade secret implications

- ☐ Understand and control remote access issues
  - Mobile devices raise tremendous data access and data breach concerns
  - Limit access
  - Control devices
  - Work with your counsel and DMS and other vendors to address the policy, security, and business implications of mobile device access.
  - Remote access from employees "home" computers
    - Also raises complicated data security, breach, trade secret and other issues
      - How do you control access/copying/sharing?
      - P2P implications? (see below)

[30] Remember that information you collect through internet "cookies" in connection with an inquiry about a financial product or service is considered NPPI. For example, if your dealership website accepts online credit applications, any information you gather during that process via cookies is NPPI.

- ☐ Consider implementing a strict data "push" system for sharing data
  - This means that you would only share data with third parties by gathering it, and sending it to them, rather than allowing them to "take" it by accessing your systems.
    - Allows you to have control over what data is shared
    - Prevents concerns regarding access to data
    - Provides audit trail of sharing
  - Work with your DMS provider to set up
  - If no/limited IT staff or expertise, consider a vendor to help.

- ☐ Implement password/access controls
  - Who has authority to grant access to the DMS, and what level of access?
  - Centralize control over password access.
    - More than one person with ability to grant password access? Why?
    - If one person, then better control over access
      - less likely to be abused
      - easier to document/demonstrate compliance
  - At the least, you must know who has a password and who is using it.
    - Work with your DMS provider to monitor and audit.
  - Address Affiliate Marketing and Sharing issues via password.
    - See NADA Guide on this complicated but important topic.
  - Prohibit employees from sharing passwords.
  - Require regular changes to passwords.
  - Require employees to use "stronger" passwords for any access to sensitive data.

- ☐ Understand "P2P"
  - "P2P" refers to "Peer-to-Peer" networks. Go here for more: http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business
  - Have a policy and train your employees.
  - Consider prohibiting access to P2P sites.

- ☐ Consider benefits of segregating your data
  - By manufacturer[31]
  - "Sensitive" from "non-sensitive"
  - Either physically (different servers/systems) or by password

- ☐ Consider the use of "dummy" or "plant" customers in your DMS

[31] It has been reported to NADA that whether due to limitations in the DMS systems themselves, or because of the way the dealer utilizes the system, dealers are sometimes unable to limit access by manufacturer. For example, a dealer who is a retailer of multiple makes for multiple manufacturers, may not be able to grant access (legitimately, pursuant to an exception to the Privacy Rule) to a manufacturer to only *that manufacturer's* customers. This creates a potential problem for the reasons described above.

  - Put a false customer in your DMS database with a physical and email address you can monitor. Then test what, if any, marketing information comes to that "customer."
  - Can provide good insight into who may be accessing your data without your knowledge.

- ☐ Understand your "Do-Not-Call" and CAN SPAM opt out procedures
  - Are your company-specific opt-out/"do-not-call" lists in place and updated?
    - Ensure that you do not share phone numbers or emails on your lists
  - How do you control third party access to phone numbers or email?

- ☐ Work with OEMs and others to limit exposure
  - Find the right person at your OEM and maintain open communication

- ☐ Understand privacy implications of your social media efforts
  - Do you gather any customer information via social media?
    - May not be NPPI, but sensitive from customer relations perspective
  - Do you have any interaction with customer comments/dealership reviews?
    - Understand the FTC Guidelines on Endorsements and Testimonials.
  - Do you engage the services of a "reputation management" vendor?
    - Understand *exactly* what they are doing, what they have access to.

- ☐ Confirm that your Privacy Notice is accurate!
  - If you share with service providers, you must properly disclose.
    - Note that this is separate from the sharing/opt-out requirement
  - Use the Model Privacy Notice form
  - Review "A Dealer Guide to the Privacy Rule and Model Privacy Notice"
    - At www.nadauniversity.com
    - Make sure you are properly using the model notice form

- ☐ Understand and meet your Affiliate Sharing and Marketing requirements
  - Applies if you have multiple legal entities (LLC, c corp. etc.)
  - Raises complicated and potentially difficult issues
  - Requires you to limit access to /use of customer data between affiliated entities
  - Review NADA Guides / consult with your attorney

See here for more details:
www.nadauniversity.com
http://business.ftc.gov/privacy-and-security/data-security
http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act
http://www.business.ftc.gov/documents/bus64-ftcs-privacy-rule-and-auto-dealers-faqs